(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. Februar 2001 (01.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/08435 A1

(51) Internationale Patentklassifikation[7]: H04Q 7/38

(21) Internationales Aktenzeichen: PCT/CH99/00336

(22) Internationales Anmeldedatum:
21. Juli 1999 (21.07.1999)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: SWISSCOM AG [CH/CH]; Alte Tiefenaustrasse 6, CH-3050 Bern (CH).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: HUBER, Adriano [CH/CH]; Via F. Caponelli, 35, CH-6600 Locarno (CH).

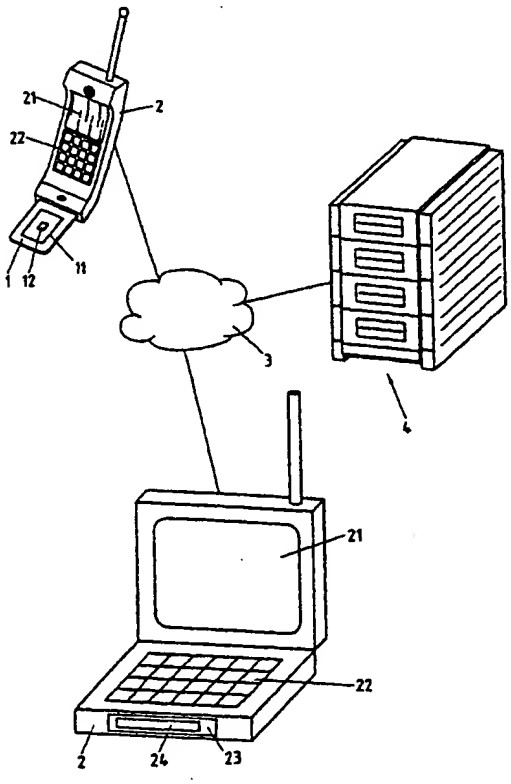
(74) Anwalt: BOVARD AG; Optingenstrasse 16, CH-3000 Bern 25 (CH).

(81) Bestimmungsstaaten *(national)*: AE, AL, AM, AT, AT (Gebrauchsmuster), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Gebrauchsmuster), DE, DE (Gebrauchsmuster), DK, DK (Gebrauchsmuster), EE, EE (Gebrauchsmuster), ES, FI, FI (Gebrauchsmuster), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND ASSOCIATED DEVICES FOR SETTING THE SECURITY LEVEL OF CRYPTOGRAPHIC FUNCTIONS

(54) Bezeichnung: VERFAHREN UND GEEIGNETE VORRICHTUNGEN, UM DEN SICHERHEITSGRAD VON KRYPTOGRAPHIEFUNKTIONEN ZU SETZEN



(57) Abstract: The invention relates to a method and associated devices for setting the security level of cryptographic functions (11, 23) used in communication terminals (2) according to situation. In a telecommunication terminal (2), especially in a mobile telephone (2), situation parameters, such as an identification code of a country where the telecommunication terminal (2) is temporarily present, are received in a secured manner from a secure source (3, 4) via a telecommunication network (3), especially a mobile telephone network (3). In addition, in said telecommunication network (2), security parameters, such as the maximum acceptable length (in bits) of cryptographic keys, are determined on the basis of the received situation parameters, and said security parameters are used by the cryptographic functions (11, 23) and determine the security level.

(57) Zusammenfassung: Verfahren und geeignete Vorrichtungen, um den Sicherheitsgrad von in Kommunikationsendgeräten (2) verwendeten Kryptographiefunktionen (11, 23) situationsabhängig zu setzen, wobei in einem Kommunikationsendgerät (2), insbesondere einem Mobilfunkgerät (2), situationsanzeigende Parameter, beispielsweise ein Ländercode des Landes, in welchem sich das Kommunikationsendgerät (2) momentan befindet, von einer sicheren Quelle (3, 4) gesichert über ein Telekommunikationsnetz (3), insbesondere ein Mobilfunknetz (3), entgegengenommen werden, und wobei im Kommunikationsendgerät (2) basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter, beispielsweise die maximal zulässige (Bit-) Länge von kryptographischen Schlüsseln, bestimmt werden, welche Sicherheitsparameter von den Kryptographiefunktionen (11, 23) verwendet werden und den Sicherheitsgrad bestimmen.

WO 01/08435 A1

SK (Gebrauchsmuster), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *Mit internationalem Recherchenbericht.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren und geeignete Vorrichtungen, um den Sicherheitsgrad von Kryptographiefunktionen zu setzen

Die vorliegende Erfindung betrifft ein Verfahren und geeignete Vorrichtungen, um den Sicherheitsgrad von Kryptographiefunktionen zu setzen. Insbesondere betrifft die vorliegende Erfindung ein Verfahren und geeignete Vorrichtungen, um den Sicherheitsgrad von in Kommunikationsendgeräten verwendeten Kryptographiefunktionen zu setzen.

Um vertrauliche Daten bei der Übertragung über Telekommunikationsnetze, insbesondere bei der Übertragung über Mobilfunknetze, vor dem Zugriff durch unberechtigte Drittparteien zu schützen ist es heutzutage allgemein üblich, Kryptographieverfahren einzusetzen, mittels welchen die vertraulichen Daten vor der Übertragung über das Telekommunikationsnetz beim Sender verschlüsselt und nach der Übertragung über das Telekommunikationsnetz beim Empfänger entschlüsselt werden. Verschiedene Kryptographieverfahren weisen unterschiedliche Sicherheitsgrade auf, die von Sicherheitsparametern, wie den verwendeten Kryptographiealgorithmen und den darin verwendeten kryptographischen Schlüsseln, insbesondere der Bitlänge der darin verwendeten Schlüssel, abhängen. Die Anwender der Kryptographieverfahren, beispielsweise Dienstleister wie Finanzinstitute oder Dienstleistungsnehmer wie Bankkunden, wünschen im Allgemeinen einen hohen Sicherheitsgrad. Allerdings gebieten nationale Interessen von gewissen Ländern, in denen beispielsweise betreffende kryptographische Produkte hergestellt werden und/oder in denen Eigentümer von entsprechenden Schutzrechten beheimatet sind, die Verbreitung von Kryptographieprodukten, beispielsweise ab gewissen vordefinierten Sicherheitsgraden oder unter Verwendung von gewissen vordefinierten Sicherheitsparametern, über die Landesgrenzen hinweg oder zumindest in gewisse definierte Länder zu unterbinden. Für die Hersteller von solchen Kryptographieprodukten, die in ihrem eigenen wirtschaftlichen Interesse ihre Produkte möglichst weltweit vermarkten möchten, die aber den nationalen Vorschriften und gesetzlichen Bestimmungen unterliegen, stellt sich nun das Problem, wie sie ihre eigenen Interessen unter Einhaltung der nationalen Bestimmungen möglichst effizient verfolgen können. Die Herstellung, Verwaltung und Wartung von verschiedenen Kryptographieprodukten für verschiedene

Märkte erweist sich dabei als keine optimale Lösung, da die Produkteversionen und insbesondere auch Kombinationen mit anderen Produkten, in welche die Kryptographieprodukte integriert werden, viel zu zahlreich sind und einen unwirtschaftlichen Mehraufwand mit sich bringen. In alternativen Lösungen wird zwar das gleiche Produkt überallhin ausgeliefert, aber gewisse Teile, die den national auferlegten Restriktionsbestimmungen unterliegen, werden vor der Produktauslieferung durch Schalter deaktiviert, beispielsweise mittels softwaremässigen Schaltern, die durch Setzen von sogenannten Flags ein- respektive ausgeschaltet werden. Das Problem dieser alternativen Lösung besteht darin, dass diese Schalter oft auch durch Drittparteien verändert werden können, beispielsweise durch sogenannte Programmpatches, die die erwähnten Flags manipulieren können.

Es ist eine Aufgabe dieser Erfindung, ein neues und besseres Verfahren sowie dafür geeignete Vorrichtungen vorzuschlagen, welche es ermöglichen, den Sicherheitsgrad von in Kommunikationsendgeräten verwendeten Kryptographiefunktionen, insbesondere situationsabhängig, zu setzen.

Gemäss der vorliegenden Erfindung wird dieses Ziel insbesondere durch die Elemente der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

Dieses Ziel wird durch die vorliegende Erfindung insbesondere dadurch erreicht, dass in einem Kommunikationsendgerät, welches über Telekommunikationsnetze kommuniziert, situationsanzeigende Parameter von einer sicheren Quelle, die beispielsweise mittels einem digitalen Zertifikat als sichere Quelle authentifiziert wird, gesichert über das Telekommunikationsnetz entgegengenommen werden, beispielsweise direkt, ohne Beeinflussungsmöglichkeiten durch andere Elemente, aus einem chiffrierten Datenobjekt mit zertifiziertem Schlüssel oder als nicht beeinflussbarer Bestandteil des im betreffenden Telekommunikationsnetz verwendeten Protokolls, und dass im Kommunikationsendgerät basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter, zum Beispiel die maximal zulässige Länge von kryptographischen Schlüsseln oder zugelassene

kryptographische Algorithmen, bestimmt werden, welche Sicherheitsparameter von Kryptographiefunktionen verwendet werden und den Sicherheitsgrad bestimmen. Der Vorteil dieses Verfahrens besteht darin, dass der Sicherheitsgrad von im Kommunikationsendgerät verwendeten Kryptographiefunktionen, respektive von diesen Kryptographiefunktionen verwendete Sicherheitsparameter, situationsabhängig und dynamisch gesetzt werden kann/können, so dass keine unterschiedlichen Kryptographieprodukte in verschiedene Zielmärkte geliefert werden müssen und vom Hersteller keine Schalter statisch gesetzt werden müssen, deren Wirkung durch ein einmaliges Überschreiben rückgängig gemacht werden kann.

In einer Ausführungsvariante enthalten mindestens gewisse situationsanzeigende Parameter dienstspezifische Angaben, beispielsweise Angaben betreffend den Typ des betreffenden Dienstes, die von einem Dienstserver, beispielsweise ein E-Mail-Server oder ein File-Transfer-Server, von welchem das genannte Kommunikationsendgerät Dienste bezieht, gesichert, beispielsweise verschlüsselt und/oder als Bestandteil eines digitalen, chiffrierten Datenobjekts mit zertifiziertem Schlüssel, über das Telekommunikationsnetz an das Kommunikationsendgerät übertragen werden. Der Vorteil, dienstspezifische Angaben bei der Festlegung des Sicherheitsgrades von Kryptographiefunktionen zu berücksichtigen besteht darin, dass verschiedene Sicherheitsgrade für unterschiedliche Dienste, beispielsweise höhere Sicherheitsgrade für Finanzdienste als für E-Mail-Dienste, für verschiedene Ebenen von Diensten, beispielsweise unterschiedliche Sicherheitsgrade auf der Transportebene und auf der Applikationsebene, und für verschiedene Anwendungen von Diensten, beispielsweise unterschiedliche Sicherheitsgrade für File-Transfer in einer Finanzanwendung (Finanzdienst) als in einer Datenbankanwendung (Datendienst) vorgeschrieben und gesetzt werden können.

In einer Ausführungsvariante enthalten mindestens gewisse situationsanzeigende Parameter Angaben über den zulässigen Sicherheitsgrad, beispielsweise gemäss einer international vereinbarten Norm oder zulässige Sicherheitsparameter, beispielsweise Angaben über spezifische zugelassene kryptographische Algorithmen, die von einem Dienstserver, von welchem das

Kommunikationsendgerät Dienste bezieht, gesichert, beispielsweise verschlüsselt und/oder als Bestandteil eines digitalen, chiffrierten Datenobjekts mit zertifiziertem Schlüssel, über das Telekommunikationsnetz an das Kommunikationsendgerät übertragen werden.

In einer Ausführungsvariante sind mindestens gewisse der Kommunikationsendgeräte Mobilfunkgeräte, beispielsweise Mobilfunktelefone oder kommunikationsfähige Lap- oder Palmtop-Computer für GSM- (Global System for Mobile Communication), UMTS- (Universal Mobile Telephone System), oder andere, beispielsweise satellitenbasierte, Mobilfunknetze und mindestens gewisse situationsanzeigende Parameter enthalten einen Ländercode, der von einem Mobilfunknetz, in welchem das Mobilfunkgerät roamt, an das Mobilfunkgerät übertragen wird. Die Anwendung des erfindungsgemässen Verfahrens in Mobilgeräten, insbesondere unter Verwendung von Ländercodes als situationsanzeigende Parameter, hat den Vorteil, dass der Sicherheitsgrad der verwendeten Kryptographiefunktionen dynamisch an die in einem betreffenden Aufenthaltsland geltenden Restriktionen betreffend zulässiger maximalen Sicherheitsgrade angepasst werden können.

An dieser Stelle soll erwähnt werden, dass sich die vorliegende Erfindung neben dem erfindungsgemässen Verfahren auch auf ein erfindungsgemässes Kommunikationsendgerät, insbesondere auf ein mobiles Kommunikationsendgerät, beispielsweise ein Mobilfunktelefon oder ein kommunikationsfähiger Lap- oder Palmtop-Computer für GSM-, UMTS- oder andere, beispielsweise satellitenbasierte, Mobilfunknetze, auf eine erfindungsgemässe Chipkarte, beispielsweise eine SIM-Karte (Subscriber Identification Module), die in einem Kommunikationsendgerät eingesetzt werden kann, sowie auf einen erfindungsgemässen Computer-lesbaren Datenträger und auf ein erfindungsgemässes Computerprogrammelement bezieht.

Nachfolgend wird eine Ausführung der vorliegenden Erfindung anhand eines Beispieles beschrieben. Das Beispiel der Ausführung wird durch folgende einzige beigelegte Figur illustriert:

Figur 1 zeigt ein Blockdiagramm mit einer schematischen Darstellung eines ersten Mobilfunkgeräts mit einer Chipkarte, eines zweiten Mobilfunkgeräts sowie eines Dienstservers, die mit einem Mobilfunknetz verbunden sind.

In der Figur 1 bezieht sich die Bezugsziffer 3 auf ein Telekommunikationsnetz, insbesondere ein Mobilfunknetz 3, beispielsweise ein GSM-, UMTS, oder ein anderes, zum Beispiel ein satellitenbasiertes, Mobilfunknetz 3, über welches Kommunikationsendgeräte 2, insbesondere Mobilfunkgeräte 2, miteinander oder mit Dienstservern 4, beispielsweise ein File-Transfer-Server, ein Finanzserver, ein Datenbankserver, oder ein E-Mail-Server, kommunizieren, das heisst insbesondere auch Daten austauschen, können.

Die Mobilfunkgeräte 2 umfassen ein erfindungsgemässes Sicherheitsgradbestimmungsmodul 12, 24, welches vorzugsweise ein programmiertes Softwaremodul ist, das sich in einem geeigneten, von Benutzern nicht manipulierbaren Speicher im Mobilfunkgerät 2 oder auf einer mit dem Mobilfunkgerät 2 verbundenen Chipkarte 1 befindet. Das Sicherheitsgradbestimmungsmodul 12, 24 ist beispielsweise Bestandteil von Kryptographiefunktionen 11, 23, die in den Mobilfunkgeräten 2 verwendet werden. Funktionen des Sicherheitsgradbestimmungsmoduls 12, 24 werden in einem Prozessor im Mobilfunkgerät 2 oder auf der mit dem Mobilfunkgerät 2 verbundenen Chipkarte 1 ausgeführt.

Die Hauptfunktion des Sicherheitsgradbestimmungsmoduls 12, 24 besteht darin, den Sicherheitsgrad der im Mobilfunkgerät 2 verwendeten Kryptographiefunktionen 11, 23, respektive von diesen Kryptographiefunktionen 11, 23 verwendete Sicherheitsparameter situationsabhängig zu setzen. Die aktuelle Situation wird dabei von sogenannten situationsanzeigenden Parametern bestimmt, welche vom Sicherheitsgradbestimmungsmodul 12, 24 von sicheren Quellen gesichert entgegengenommen werden.

Als situationsanzeigende Parameter gelten beispielsweise das betreffende Land, in welchem das Mobilfunkgerät 2 betrieben wird, oder dienstspezifische Angaben, beispielsweise der betreffende Dienst oder Diensttyp eines Dienstservers 4, welcher vom Mobilfunkgerät 2 benutzt wird, oder Anga-

ben betreffend Protokolle, respektive Protokollebenen, die von diesem Dienst verwendet werden oder andere Angaben über den betreffenden Dienst, respektive Angaben darüber, wie ein bestimmter Dienst, respektive eine verfügbare Funktion, angewendet wird, beispielsweise kann für die Verwendung von File-Transfer-Funktionen in einer Finanzanwendung (Finanzdienst) ein höherer Sicherheitsgrad zulässig sein als für deren Verwendung in einer Datenbankanwendung (Datendienst). Es ist auch möglich, dass die situationsanzeigenden Parameter direkte und spezifische Angaben betreffend den zu verwendenden Sicherheitsparametern oder des maximal zulässigen und/oder zu verwendenden Sicherheitsgrades enthalten, wobei Angaben betreffend den Sicherheitsgrad vorzugsweise auf einer internationalen Norm beruhen.

Als Sicherheitsparameter gelten beispielsweise die (Bit-) Länge von verwendeten kryptographischen Schlüsseln oder die Benennung von spezifischen zu verwendenden kryptographischen Algorithmen aus einer Reihe von möglichen alternativen Algorithmen.

Eine Quelle von situationsanzeigenden Parametern, beispielsweise der Dienstserver 4, kann beispielsweise dann als sicher akzeptiert werden, wenn von ihr ein digitales (signiertes) Zertifikat erhalten wird, welches die Quelle authentifiziert. Die Netzwerkinfrastruktur des Mobilfunknetzes 3 kann in dem Sinne als sichere Quelle betrachtet werden, als nicht beeinflussbare Bestandteile des im Mobilfunknetz 3 verwendeten Protokolls als situationsanzeigende Parameter verwendet werden.

Situationsanzeigende Parameter werden in dem Sinne gesichert über das Telekommunikationsnetz entgegengenommen, als sie direkt, ohne Beeinflussungsmöglichkeiten durch andere Elemente, beispielsweise aus einem digitalen, chiffrierten Datenobjekt mit zertifiziertem Schlüssel oder als nicht beeinflussbarer Bestandteil aus Protokolldateneinheiten des im betreffenden Mobilfunknetz 3 verwendeten Protokolls entnommen werden.

Zur Umsetzung von entgegengenommenen situationsanzeigenden Parametern in zu verwendende Sicherheitsparameter verfügt das Sicherheitsgradbestimmungsmodul 12, 24 beispielsweise über entsprechende, vom Be-

nutzer nicht manipulierbare Tabellen oder entsprechende Programminstruktionen, mittels welchen den aktuellen entgegengenommenen situationsanzeigenden Parametern entsprechende Sicherheitsparameter zugeordnet werden. Da sich die zulässigen Sicherheitsgrade, respektive Sicherheitsparameter, insbesondere in verschiedenen Ländern im Laufe der Zeit ändern können, ist es möglich, diese Tabellen, respektive diese Programminstruktionen, unter Zuhilfenahme von sicheren kryptographischen Funktionen in einem zuständigen Dienstleistungszentrum oder über das Mobilfunknetz 3 zu aktualisieren.

Situationsanzeigende Parameter werden vom Sicherheitsgradbestimmungsmodul 12, 24 beispielsweise dadurch erfasst, dass über das Mobilfunknetz 3 empfangene Protokolldateneinheiten darauf überprüft werden, ob sie einen neuen Ländercode enthalten (MCC, Mobile Country Code), oder dass über das Mobilfunknetz 3 empfangene, chiffrierte Datenobjekte mit zertifiziertem Schlüssel (digitale Zertifikate) darauf geprüft werden, ob sie situationsanzeigende Parameter enthalten, zum Beispiel dienstspezifische Angaben wie beispielsweise eine Angabe betreffend den aktuellen Diensttyp, zum Beispiel E-Mail oder File-Transfer, oder betreffend die Anwendung eines Dienstes, beispielsweise die Verwendung von File-Transfer in einer Finanzanwendung (Finanzdienst) oder in einer Datenbankanwendung (Datendienst). Der Fachmann wird verstehen, dass es auch möglich ist, für die Bestimmung von situationsanzeigenden Parametern, respektive für die Bestimmung von Sicherheitsgraden und/oder den zu verwendenden Sicherheitsparametern spezielle Protokolle zu definieren, die zwischen Kommunikationsendgeräten 2, insbesondere den darin enthaltenen Sicherheitsgradbestimmungsmodul 12, 24 und Dienstservern 4 eingesetzt werden können.

Es soll hier auch erwähnt werden, dass situationsanzeigende Parameter und die Differenzierung der zu verwendenden Sicherheitsgrade, respektive Sicherheitsparameter, auch individuelle Protokollebenen betreffen können, beispielsweise Protokollebenen gemäss dem siebenschichtigen OSI-Referenzmodell (Open Systems Interconnection) der ISO (International Standards Organisation), so dass beispielsweise für die Applikationsebene (OSI-Schicht 7) und die Transportebene (OSI-Schicht 4) verschiedene Restriktionen betreffend zulässige Sicherheitsgrade anwendbar sind. Es sollte auch erwähnt wer-

den, dass typischerweise mehrere situationsanzeigende Parameter kombiniert werden, so dass beispielsweise im Land „X" und im Land „Y" die gleichen Restriktionen auf der Transportebene gelten können, aber für das Land „X" strengere Restriktionen auf der Applikationsebene gelten als für das Land „Y".

Änderungen des Sicherheitsgrades der im Mobilfunkgerät 2 verwendeten Kryptographiefunktionen 11, 23, respektive von diesen Kryptographiefunktionen 11, 23 verwendeten Sicherheitsparametern, können dem Benutzer, beispielsweise durch programmierte Funktionen des Sicherheitsgradbestimmungsmoduls 12, 24, mittels der Anzeige 21 mitgeteilt werden. Es ist auch möglich, dass sich der Benutzer des Mobilfunkgeräts 2 selber über aktuelle Sicherheitsgrade, respektive momentan verwendete Sicherheitsparameter, informieren kann, indem er beispielsweise entsprechende programmierte Funktionen des Sicherheitsgradbestimmungsmoduls 12, 24 aktiviert, zum Beispiel mittels der Bedienungselemente 22 des Mobilfunkgeräts 2.

Neben den eingangs erwähnten Vorteilen für die Hersteller von Produkten mit kryptographischen Funktionen (11, 23) ergeben sich auch Möglichkeiten, die vorliegende Erfindung wirtschaftlich direkt zu vermarkten. Zum Beispiel können Kommunikationsendgeräte und/oder Chipkarten hergestellt und verkauft werden, die ein erfindungsgemässes Sicherheitsgradbestimmungsmodul umfassen. Es ist auch möglich Computer-lesbare Datenträger herzustellen und zu verkaufen, oder unter Lizenzgebühren abzugeben, welche Datenträger codierte Daten enthalten, die ein Computer-Programm repräsentieren, welches Computer-Programm ermöglicht, einen Prozessor, insbesondere in einem Kommunikationsendgerät, so zu steuern, dass er den Sicherheitsgrad von verwendeten Kryptographiefunktionen (11, 23), respektive von diesen Kryptographiefunktionen (11, 23) verwendete Sicherheitsparameter, gemäss dem beschriebenen Verfahren situationsabhängig setzt. Computerprogrammelemente, die Computerprogrammcodemittel umfassen, um einen Prozessor, insbesondere in einem Kommunikationsendgerät, so zu steuern, dass er den Sicherheitsgrad von verwendeten Kryptographiefunktionen (11, 23), respektive von diesen Kryptographiefunktionen (1, 23) verwendete Sicherheitsparameter, gemäss dem beschriebenen Verfahren situationsabhängig setzt, können gegen Bezahlung von Lizenzgebühren an Dritte abgegeben werden, welche diese

Computerprogrammelemente in verschiedenste Vorrichtungen integrieren können.

Liste der Bezugszeichen

1 Chipkarte (SIM-Karte)

2 Kommunikationsendgerät (Mobilfunkgerät)

3 Telekommunikationsnetz (Mobilfunknetz)

4 Dienstserver

11 Kryptographiefunktionen

12 Sicherheitsgradbestimmungsmodul

21 Anzeige

22 Bedienungselemente

23 Kryptographiefunktionen

24 Sicherheitsgradbestimmungsmodul

Ansprüche

1. Verfahren um den Sicherheitsgrad von in Kommunikationsendgeräten (2) verwendeten Kryptographiefunktionen (11, 23) zu setzen, welche Kommunikationsendgeräte (2) über Telekommunikationsnetze (3) kommunizieren, dadurch gekennzeichnet,

dass in einem genannten Kommunikationsendgerät (2) situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegengenommen werden, und

dass im genannten Kommunikationsendgerät (2) basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt werden, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11, 23) verwendet werden und den genannten Sicherheitsgrad bestimmen.

2. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass mindestens gewisse genannte situationsanzeigende Parameter dienstspezifische Angaben enthalten, die von einem Dienstserver (4), von welchem das genannte Kommunikationsendgerät (2) Dienste bezieht, gesichert über das Telekommunikationsnetz (3) an das genannte Kommunikationsendgerät (2) übertragen werden.

3. Verfahren gemäss einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass mindestens gewisse genannte situationsanzeigende Parameter Angaben über den zulässigen Sicherheitsgrad oder zulässige Sicherheitsparameter enthalten, die von einem Dienstserver (4), von welchem das genannte Kommunikationsendgerät (2) Dienste bezieht, gesichert über das Telekommunikationsnetz (3) an das genannte Kommunikationsendgerät (2) übertragen werden.

4. Verfahren gemäss einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass mindestens gewisse genannte Kommunikationsendgeräte (2) Mobilfunkgeräte sind, und dass mindestens gewisse genannte situationsanzei-

gende Parameter einen Ländercode enthalten, der von einem Mobilfunknetz (3), in welchem das genannte Mobilfunkgerät (2) roamt, an das genannte Mobilfunkgerät (2) übertragen wird.

5. Verfahren gemäss einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass ein genannter Sicherheitsparameter die maximal zulässige Länge von kryptographischen Schlüsseln angibt.

6. Verfahren gemäss einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass ein genannter Sicherheitsparameter Angaben über zulässige kryptographische Algorithmen enthält.

7. Kommunikationsendgerät (2), das über ein Telekommunikationsnetz (3) kommuniziert, dadurch gekennzeichnet,

dass das Kommunikationsendgerät (2) ein Sicherheitsgradbestimmungsmodul (12, 24) umfasst, um den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11, 23) situationsabhängig zu setzen, welches Sicherheitsgradbestimmungsmodul (12, 24) situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, und welches Sicherheitsgradbestimmungsmodul (12, 24) basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11, 23) verwendet werden und den genannten Sicherheitsgrad bestimmen.

8. Chipkarte (1), die entfernbar mit einem Kommunikationsendgerät (2) verbunden werden kann, welches Kommunikationsendgerät (2) über ein Telekommunikationsnetz (3) kommuniziert, dadurch gekennzeichnet,

dass die Chipkarte (1) ein Sicherheitsgradbestimmungsmodul (12) umfasst, um den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11) situationsabhängig zu setzen, welches Sicherheitsgradbestimmungsmodul (12) situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3)

entgegennimmt, und welches Sicherheitsgradbestimmungsmodul (12) basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11) verwendet werden und den genannten Sicherheitsgrad bestimmen.

9. Computer-lesbarer Datenträger, der codierte Daten enthält, die ein Computer-Programm repräsentieren, welches Computer-Programm ermöglicht, einen Prozessor in einem Kommunikationsendgerät (2), welches Kommunikationsendgerät (2) über ein Telekommunikationsnetz (3) kommuniziert, so zu steuern, dass er den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11, 23) situationsabhängig setzt, wobei er situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, und wobei er basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11, 23) verwendet werden und den genannten Sicherheitsgrad bestimmen.

10. Computerprogrammelement umfassend: Computerprogrammcodemittel, um einen Prozessor in einem Kommunikationsendgerät (2), welches Kommunikationsendgerät (2) über ein Telekommunikationsnetz (3) kommuniziert, so zu steuern, dass er den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11, 23) situationsabhängig setzt, wobei er situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, und wobei er basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11, 23) verwendet werden und den genannten Sicherheitsgrad bestimmen.

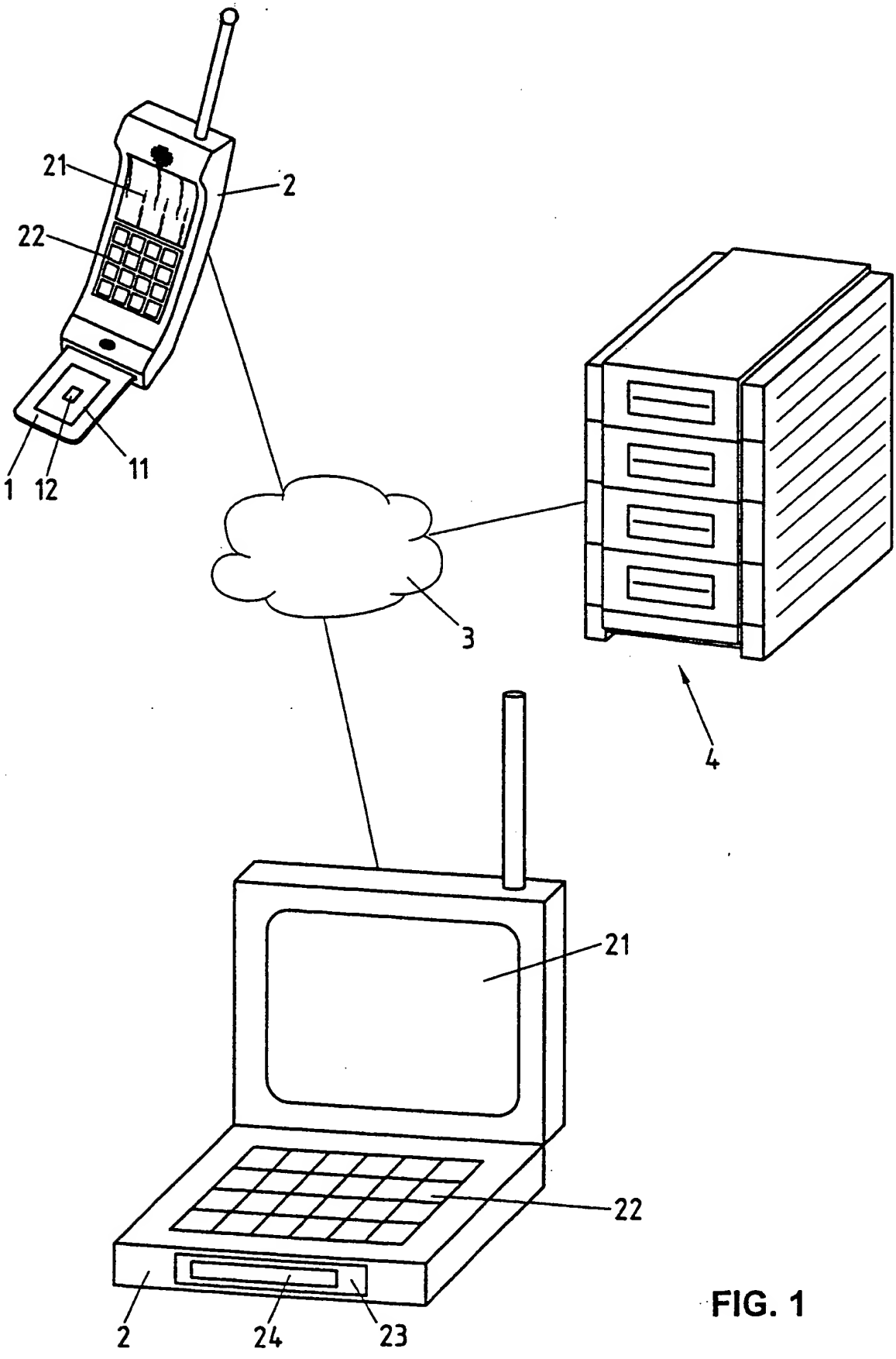


FIG. 1